# Fac-simile documento programmatico sulla sicurezza nel trattamento dei dati personali

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dallo Studio Legale _____
Il presente documento è stato redatto da_____in qualità di titolare / responsabile per la sicurezza, che provvede a firmarlo in calce.

## Elenco dei trattamenti di dati personali

Lo Studio Legale tratta i seguenti dati:
- dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;
- dati comuni del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;
- dati comuni dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati comuni di terzi, forniti dai clienti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari;
- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;
- dati comuni di altri Avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;
- dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;
- dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;
- dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;
- dati sensibili dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;
- dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;
- dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;
- dati sensibili di clienti o terzi, comunque afferenti la vita sessuale.

I dati non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S.
Questi dati vengono trattati e conservati in fascicoli riposti in schedari dotati di chiusura, nonché trattati tramite computer in rete in locali protetti e con accesso ad internet, archiviati al termine della pratica.
Lo studio, ove vengono trattati i dati, è ubicato in un condominio in zona centrale, dotato di portone di ingresso a chiusura automatica e con videocitofono, con sorveglianza notturna, e porte blindate. Sito al primo piano. I singoli studi, che lo compongono, sono dotati ciascuno di porta con chiusura a chiave, così come l'archivio. La segreteria è ubicata in un locale più ampio, dove in una zona separata e ben distanziata dalle postazioni di lavoro delle segretarie, è ricavata una sala di attesa per i clienti.
Lo studio è dotato di cassaforte con chiusura a chiave.
Ogni studio è dotato di un computer in rete e connesso ad internet con connessione ADSL in rete, eccezione fatta per la sala biblioteca dove sono ubicati due computer in rete e con connessione ADSL ad internet; nel più ampio locale, ove è ubicata la segreteria si trovano due postazioni di lavoro con computer con connessione ADSL ad internet ed in fianco ad una di esse è ubicato il server connesso ad internet ed il router per la connessione ad internet. Inoltre in questo locale si trovano le stampanti, il fax, la fotocopiatrice e lo scanner. Uno dei due computer è dotato di separato modem per l'utilizzo di Winfax. Le linee telefoniche sono due ISDN.
Il sistema operativo del server è ……..
Il sistema operativo dei computer è……
Lo studio adopera Internet Explorer versione …..
Lo studio adopera OutlooK Express ……..
Lo studio per adopera per a gestione il sistema……
Antivirus adoperato …….
Firewall adoperato …….
Titolare del trattamento è l'avv……..
Responsabile del trattamento è ……
Amministratore del sistema è …….
Incaricati del trattamento sono:
Dr. …… (collaboratore di studio)
Dr. …… (collaboratore di studio)
……. (dipendente)
…….. (dipendente)

Tecnico incaricato dell'assistenza e manutenzione degli strumenti elettronici è …….

I dati comuni dei clienti, dei fornitori o di terzi, i dati comuni di altri Avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, i dati giudiziari dei clienti, i dati giudiziari di terzi, i dati sensibili dei clienti e di terzi sono trattati, oltre che dal titolare, anche da tutti gli incaricati.
I dati comuni del personale dipendente, i dati sensibili del personale dipendente, i dati afferenti i pagamenti a favore di terzi fornitori, la

contabilità e i rapporti bancari dello studio sono esclusivamente tenuti dalla dipendente……., che si occupa della amministrazione. Questi dati non sono in rete ma si trovano solo sul computer della segretaria autorizzata a trattarli.

E' stata compiuta l'analisi dei rischi che si può così sintetizzare:
per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni dei clienti (dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari) i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) i dati comuni di altri avvocati e professionisti cui lo studio affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali: il rischio legato alla loro gestione può definirsi basso/medio
Per i dati sensibili del personale dipendente, i dati giudiziari dei clienti,i dati giudiziari di terzi, i dati sensibili dei clienti (dagli stessi forniti per l'espletamento degli incarichi affidati allo studio) i dati sensibili di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio) il rischio legato alla loro gestione è da definirsi medio, eccezion fatta per i dati riguardanti le pratiche in cui sono contenuti dati idonei a rivelare lo stato di salute, o dati giudiziari di clienti o terzi e le pratiche, quali quelle in materia di diritto familiare, con dati idonei a rivelare la vita sessuale. Per questi ultimi dati il rischio collegato alla gestione può definirsi alto. Per i dati sensibili afferenti cause di stato (esempio disconoscimento di paternità) il rischio di gestione può essere definito maggiormente elevato.

Gli strumenti elettronici sono:
nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da ……. marca …….. modello ……
nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da …….. marca …….. modello …..
nr. 1 computer server connesso in rete ed a internet nella segreteria marca ……. modello ……
nr. 1 computer connesso in rete ed a internet nello studio dell'avv. ……. utilizzato dallo stesso marca ….. modello ……
nr. 1 computer connesso in rete ed a internet nello studio dell'avv. ……. utilizzato dallo stesso marca …… modello …….
nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da …….. marca ……. modello ……..

nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da …….. marca ……. modello ……..
Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, alterazioni delle trasmissioni.
Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.
Per quanto riguarda le aree ed i locali: possono essere colpiti da eventi naturali o accessi di terzi non autorizzati.

Per ridurre i rischi sono state adottate le seguenti misure:
Autenticazione informatica, tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri ( o minore per le caratteristiche del sistema). Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né allo studio legale. La stessa viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al titolare del trattamento, il quale provvede a metterla nella cassaforte dello studio in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Si è altresì disposto che le password vengano automaticamente disattivate dopo tre mesi di non utilizzo.
Inoltre si è disposto che a tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.
A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo screensaver automatico dopo 1 minuto di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
Si è inoltre disposto che essi verifichino la provenienza delle email e non operino operazioni di sharing.
Essendo gli incaricati autorizzati a trattare la quasi totalità dei dati, e comunque quelli sensibili e giudiziari, non si è provveduto a dare disposizioni in caso di prolungata assenza o impedimento dell'incaricato, eccezion fatta per i dati trattati in via esclusiva dal dipendente ……, che cura la contabilità, per il quale è stato indicato per iscritto il nominativo dell'incaricato della sostituzione.
Ogni singolo computer è dotato di dispositivo antivirus di marca ……., che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e comunque settimanale.
Sul server è stato installato firewall di marca …….
Per ogni singolo computer è prevista la funzione di aggiornamento automatico del sistema fornito dalla Microsoft mediante lo strumento windows – update.
Analogo sistema di aggiornamento automatico è previsto per l'antivirus. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di mesi 6, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.

E’ stato disposto l’obbligo di provvedere ad un backup settimanale dei dati e dei sistemi installati sul server su cd rom, i quali vengono conservati e chiusi in un cassetto, e si è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati; custode di detti backup è stato nominato l’incaricato …… Si è data disposizione che, effettuato un backup, venga distrutto il c.d. precedente.
Si è data disposizione che, terminata la trattazione di una pratica, ogni relativo file, o dato, esistente sui computer, sia cancellato.
Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.
Le comunicazioni a mezzo posta, o a mezzo telefax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all’interessato.
Il locale destinato all’archivio dovrà essere chiuso a chiave. La dipendente …….. è incaricata di controllare l’accesso all’archivio. Fuori dall’orario di lavoro l’accesso all’archivio è consentito previa registrazione.
Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica e che detti sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.
Il rischio di accesso ai locali dello studio, può essere definito basso, atteso che l’ingresso allo studio è controllato, e che lo studio è dotato di videocitofono e chiusura con porta blindata.
Il rischio di accesso ai singoli studi può essere definito basso, atteso che gli stessi sono dotati di porte con chiusura e l’ingresso di terzi estranei avviene solo previa accettazione e controllo.
Il rischio di accesso ai singoli strumenti da parte di persone non autorizzate può essere definito basso, essendo controllato l’accesso allo studio da parte di terzi; la zona di attesa dei clienti distanziata dagli strumenti ed essendo gli stessi clienti controllabili dalla segreteria.
Le aree ed i locali potrebbero essere interessati da eventi naturali, quali incendi, allagamenti e corto circuiti, pur avendo lo studio provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94. Essendo lo studio dotato di dispositivi salvavita, il rischio può comunque definirsi basso.
Per quanto riguarda gli strumenti elettronici, il rischio può essere definito basso, essendo state adottate dallo studio le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.
Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo l’archivio chiuso a chiave, gli schedari chiusi, ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi naturali.

I telefax inviati su carta chimica sono stati riprodotti su carta normale per evitarne il deterioramento.
Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati da essi portati può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in un cassetto chiuso a chiave, così come i dischi di installazione dei programmi software adottati.
Non vi sono elaboratori non in rete, non vi sono elaboratori non in rete e connessi ad internet, per cui nessun giudizio di rischio deve essere dato su detti strumenti.
Atteso –infine- che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio afferente la riservatezza, o la distrazione, o l'incuria degli stessi, può essere definito basso.
Inoltre i dati, quanto comuni che sensibili, per gli affari trattati dallo Studio ed il tipo di clientela dello Studio non paiono essere, come detto, di particolare interesse per terzi.
Si ritiene che verranno adottate le seguenti ulteriori misure.
Entro il termine del 30.06.2004 sarà installato sistema di firma elettronica per la trasmissione delle e-mail.
Sarà inoltre adottata ogni altra misura che dal tecnico della manutenzione venisse ritenuta utile e necessaria per migliorare la sicurezza degli strumenti elettronici.
Sarà installato inoltre gruppo di continuità per il server.
Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, si predisporrà entro il 30.06.2004 apposito piano di ripristino degli stessi, impartendosi comunque sin d'ora le seguenti istruzioni:
- avvertire il titolare del trattamento dei dati e l'incaricato che ha in custodia il c.d. di back up nonché i c.d. contenenti i vari software dello studio installati sugli strumenti elettronici;
- rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore della ditta ……. sollecitandone al più presto l'assistenza;
- reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel c.d. di back up;
- provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
- in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
- al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei datti in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.
La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.
La formazione è fatta dal titolare dello studio.
Nel caso in cui il trattamento dei dati sensibili e/o giudiziari venga affidato a soggetti esterni, che li trattino con strumenti elettronici, per avere la garanzia che essi adottano le misure minime di sicurezza si esigerà dagli stessi una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale attestino di aver adottato le misure minime previste dal disciplinare.
Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio, viene dato incarico scritto con richiesta di specificazione dei nomativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.
Si allegano oltre l'informativa, la lettera di istruzioni agli incaricati, la lettera alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio.
Teramo, lì
Il titolare
*Modello predisposto da: Avv.*